protocol overhead substantially as compared to the overhead of PEM when used in conjunction with an asymmetric key-management system.

We have also described how this scheme may be used in conjunction with datagram multicast protocols, allowing a single encrypted datagram to be multicast to all the receiving codes.

References

[1] IETF PEM RFCs 1421-1424

[2] A. Aziz, W. Diffie, "Privacy and Authentication for Wireless LANs", IEEE Personal Communications, Feb. 1994.

[3] W. Diffie, M. Wiener, P. Oarschot, "Authentication and Authenticated Key Exchanges", in Designs Codes and Cryptography, Kluwer Academic Publishers, 1991.

[4] W. Diffie, M. Hellman, "New Directions in Cryptography", IEEE Transactions on Information Theory

[5] S. Deering, "IP Multicast", Ref needed

[6] S. Kent, "Certificate Based Key Management," RFC 1422 for PEM

[7] "Public Key Cryptography Standards" 1-10 from RSA Data Security Inc., Redwood City, Calif.

Each of the above references is incorporated into this Appendix A by reference.

What is claimed:

~~1. A method for transmitting and~~ receiving packets of data via a internetwork for a first host computer on a first computer network to a second host computer on a second computer network, the first and second computer networks including, respectively, first and second bridge computers, each of said first and second host computers and first and second bridge computers including a processor and a memory for storing instructions for execution by the processor, each of said first and second

bridge computers further including memory for storing at least one predetermined encryption/decryption mechanism and information identifying a predetermined plurality of host computers as hosts requiring security for packets transmitted between them, the method being carried **[carded]** out be means of the instructions stored on said respective memories and including the steps of:

(1) generating, by the first host computer, a first data packet for transmission to the second host computer, a portion of the data packet including information representing an internetwork address of the first host computer and internetwork address of the second host computer;

(2) in the first bridge computer, intercepting the first data packet and determining whether the first and second host computers are among the predetermined plurality of host computers for which security is required, and if not, proceeding to step 5, and if so, proceeding to step 3;

(3) encrypting the first data packet in the first bridge computer;

(4) in the first bridge computer, generating and appending to the first data packet an encapsulation header, including:

(a) key management information identifying the predetermined encryption method, and

(b) a new address header representing the source and destination for the data packet, hereby generating a modified data packet;

(5) transmitting the data packet from the first bridge computer via the internetwork to the second computer network;

(6) intercepting the data packet at the second bridge computer;

(7) in the second bridge computer, reading the encapsulation header, and determining therefrom whether the data packet was encrypted, and if not, proceeding to step 10, and if so, proceeding to step 8;

(8) in the second bridge computer, determining which encryption mechanism was used to encrypt the first data packet;

(9) decrypting the first data packet by the second bridge computer;

(10) transmitting the first data packet from the second bridge computer to the second host computer, and

(11) receiving the unencrypted data packet at the second host computer.

2. The method of claim 1, wherein the new address header for the modified data packet includes the address of the second bridge computer.

3. The method of claim 2, wherein the new address header for the modified data packet includes an identifier of the second bridge computer.

4. The method of claim 1, wherein the new address header of the modified data packet includes the address of the second host computer.

5. The method of claim 4, wherein the new address header for the modified data packet includes an identifier of the second bridge computer.

6. A system for automatically encrypting and decrypting data packets transmitted from a first host computer on a first computer network to a second host computer on a second computer network, including:

a first bridge computer coupled to the first computer network for intercepting data packets transmitted from said first computer network, the first bridge computer including a first processor and a first memory storing instructions for executing encryption of data packets according to a predetermined encryption/decryption mechanism;

a second bridge computer coupled to the second computer network for intercepting data packets transmitted

to said second computer network, the second bridge computer including a second processor and a second memory storing instructions for executing decryption of the data packets;

said first host computer including a third processor and a third memory including instructions for transmitting a first said data packet from said first host to said second host;

a first table stored in said first memory including a correlation of at least one of the first host computer and the first network with one of the second host computer and the second network, respectively;

instructions stored in said first memory for intercepting said first data packet before departure from said first network, determining whether said correlation is present in said first table, and if so, then executing encryption of said first data packet according to said predetermined encryption/decryption mechanism, generating a new address header and appending said new address header to said first data packet, thereby generating a modified first data packet, and transmitting said modified first data packet on to the second host computer;

a second table stored in said second memory including a correlation of at least one of the first host computer and the first network with one of the second host computer and the second network, respectively;

instructions stored in said second memory for intercepting said first data packet upon arrival at said second network, determining whether said correlation is present in said second table, and if so, then executing decryption of said first data packet according to said predetermined encryption/decryption mechanism, and transmitting the first data packet to the second host computer.

7. The method of claim 6, wherein said new address header includes the internetwork broadcast addresses of the first and second computer networks.

8. The method of claim 7, wherein said new address header includes an identifier of the second bridge computer.

9. The method of claim 6, wherein said new address header includes the address of the second host computer.

10. The method of claim 9, wherein said new address header includes an identifier of the second bridge computer.

11. ~~A method for transmitting and~~ receiving packets of data via an internetwork from a first host computer on a first computer network to a second host computer on a second computer network, **[the first and second computer networks,]** each of said first and second host computers including a processor and a memory for storing instructions for execution by the processor, each said memory storing at least on predetermined encryption/decryption mechanism and a source/destination table identifying a predetermined plurality of sources and destinations requiring security for packets transmitted between them, the method being carried **[carded]** out by means of the instructions stored in said respective memories and including the steps of:

(1) generating, by the first host computer, a first data packet for transmission to the second host computer, a portion of the data packet including information representing an internetwork address of a source of the packet and an internetwork address of a destination of the packet;

(2) in the first host computer, determining whether the source and destination of the first data packet are among the predetermined plurality of sources and destinations identified in said source/destination table for which security is required, and if not, proceeding to step 5, and if so, proceeding to step 3;

(3) encrypting the first data packet in the first host computer;

(4) in the first host computer, generating and appending to the first data packet an encapsulation header, including:

(a) key management information identifying the predetermined encryption method, and

(b) a new address header identifying the source and destination for the first data packet;

(5) transmitting the first data packet from the first host computer via the internetwork to the second computer network;

(6) in the second host computer, reading the encapsulation header, and determining therefrom whether the first data packet was encrypted, and if not, ending the method, and if so, proceeding to step 7;

(7) in the second host computer, determining which encryption mechanism was used to encrypt the first data packet; and

(8) decrypting the first data packet by the second host computer.

12. The method of claim 11, wherein the new address header for the modified data packet includes internetwork broadcast addresses of the first and second computer networks.

13. The method of claim 11, wherein the source/destination table includes data identifying internetwork addresses of the first and second host computers.

~~14. A system for automatically encrypting~~ and decrypting data packets transmitted from a first host computer on a first computer network and having a first host computer on a first computer network and having first processor and a first memory, via an internetwork to a second host computer on a second computer network and having a second host computer on a second computer

network and having a second processor and a second memory, the system including:

security data stored in said first and second memories indicating that data packets meeting at least one predetermined criterion are to be encrypted;

a predetermined encryption/decryption mechanism stored in said first and second memories;

a decryption key stored in said second memory ;

instructions stored in said first memory for determining whether to encrypt data packets, by determining whether said at least one predetermined criterion is met by said data packet;

instructions stored in said first memory for executing encryption according to said predetermined encryption/decryption mechanism of at least a first said data packet, when said at least one predetermined criterion is met, for generating a new address header for said first data packet and for appending an encapsulation header to said first data packet and transmitting said first data packet to said second host, said encapsulation header including at least said new address header;

instructions stored in said second memory for receiving said first data packet, determining whether it has been encrypted by reference to said security data, and if so then determining which encryption/decryption mechanism was used for encryption, and decrypting said data packet by use of said decryption key.

15. The system of claim 14, wherein:

said security data comprises correlation data stored in each of said first and second memories identifying at least one of said first and second memories identifying at least one of said first host computer and said first network correlated with at least one of said second host computer and said second network;

the system further including instructions stored in said first memory for determining whether to encrypt data packets by inspecting for a match between source and

destination addresses of said data packets with said correlation data.

16. A system for automatically encrypting data packets for transmission from a first host computer on a first computer network to a second host computer on a second computer network, said first host computer including a first processor and a first memory including instructions for transmitting said data packets from said first host to said second host, the system including:

a bridge computer coupled to the first computer network for intercepting at least a first said data packet transmitted from said first computer network, said bridge computer including a second processor and a second memory storing instructions for executing encryption of said first data packet according to a predetermined encryption/decryption mechanism;

information stored in said second memory correlating at least one of the first host computer and the first network with one of the second host computer and the second network, respectively;

instructions stored in said second memory for intercepting said first data packet before departure from said first network, determining whether said correlation is present, and if so, then executing encryption of said first data packet according to said predetermined encryption/decryption mechanism, generating a new address header and appending said new address header to said first data packet, thereby generating a modified first data packet on to the second host computer.

17. A method for transmitting packets of data via an internetwork from a first host computer on a first computer network to a second host computer on a second computer network, the first computer networks including a first bridge computer, each of said first and second host computers and said bridge computer further including memory storing at least one predetermined encryption/decryption mechanism and information

identifying a predetermined plurality of host computers as hosts requiring security for packets transmitted between them, the method being carried out according to the instructions stored in said respective memories and including the steps of:

(1) generating, by the first host computer, a first data packet for transmission to the second host computer, a portion of the data packet including information representing an internetwork address of the first host computer and an internetwork address of the second host computer.

(2) in the first bridge computer, intercepting the first data packet and determining whether the first and second host computers are among the predetermined plurality of host computers for which security is required, and if not, proceeding to step 5; and if so, proceeding to step 3;

(3) encrypting the first data packet in the first bridge computer;

(4) in the first bridge computer, generating and appending to the first data packet an encapsulation header, including:

(a) key management information identifying the predetermined encryption method, and

(b) a new address header representing the source and destination for the data packet,

thereby generating a modified data packet; and

(5) transmitting the data packet from the first bridge computer via the internetwork to the second computer network.

18. A system for automatically decrypting data packets transmitted from a first computer to a second computer, the system comprising:

a bridge coupled to the second computer for intercepting a data packet from the first computer, the bridge including a processor and a memory that stores instructions for decrypting data packets;

information stored in the memory of the bridge correlating the first and second computers; and

instructions stored in the memory of the bridge for intercepting the data packet, determining whether the information stored in the memory of the bridge correlates the first and second computers, and if so, decrypting the data packet to generate a new data packet including a new address header, and transmitting the new data packet onto the second computer.

19. The system of claim 18, where the data packet includes an address header and a body, the body including the new data packet in encrypted form.

20. The method of claim 18, wherein the data packet includes a header storing key management information identifying an encryption method used to encrypt the new data packet.

21. The method of claim 18, wherein the new address header includes information indicating the first computer is a source of the new data packet and the second computer is a destination of the new data packet.

22. A method for receiving data packets transmitted from a first computer to a second computer through a bridge, the bridge including a processor and a memory, the memory storing instructions for decrypting data packets and information correlating the first and second computers, the method being carried out according to instructions in the memory of the bridge and comprising:

intercepting a data packet from the second computer to the second computer portion of the data packet including information representing an internetwork address of the first computer and an internetwork address of the second computer;

determining whether the information stored in the memory of the bridge correlates the first and second computers, and if so, decrypting the data packet to generate a new data packet including a new address header; and

transmitting the new data packet on to the second computer.

23. The system of claim 22, where the data packet includes an address header and a body, the body including the new data packet in encrypted form.

24. The method of claim 22, wherein the data packet includes a header storing key management information identifying an encryption method used to encrypt the new data packet.

25. The method of claim 22, wherein the new address header includes information indicating the first computer is a source of the new data packet and the second computer is a destination of the new data packet.

26. A method of encrypting data packets, comprising:

receiving a data packet from a source for a destination, the data packet including a header section and a data section, and the header section storing a source identifier and a destination identifier;

determining whether the data packet should be encrypted upon reference to at least one of the source and destination identifiers; and

if the data packet should be encrypted, encrypting the data packet to produce an encrypted data packet.

27. The method of claim 26, further comprising transmitting the encrypted data packet to the destination.

28. The method of claim 26, wherein the determining whether the data packet should be encrypted comprises accessing stored information that indicates by presence or absence of the source identifier that data packets from the source should be encrypted.

29. The method of claim 26, wherein the determining whether the data packet should be encrypted comprises accessing stored information that indicates by presence or absence of a correlation between the source and destination identifiers that data packets from the source for the destination should be encrypted.

30. The method of claim 26, wherein the encrypted data packet includes an encrypted data packet header section and an encrypted data packet data section, the encrypted data packet data section storing the encrypted data packet.

31. The method of claim 30, wherein the encrypted data packet header section stores the source and destination identifiers.

32. The method of claim 30, wherein the source is a host computer in a network and the encrypted data packet header section stores an identifier of the network.

33. The method of claim 30, wherein the destination is a host computer in a network and the encrypted data packet header section stores an identifier of the network.

34. The method of claim 26, wherein the source is a host computer or a network.

35. The method of claim 26, wherein the destination is a host computer or a network.

36. A computer program product for encrypting data packets, comprising:

computer code that receives a data packet from a source for a destination, the data packet including a header

section and a data section, and the header section storing a source identifier and a destination identifier;

computer code that determines whether the data packet should be encrypted upon reference to at least one of the source and destination identifiers;

computer code that encrypts the data packet to produce an encrypted data packet if the data packet should be encrypted; and

a computer readable medium that stores the computer codes.

37. The computer program product of claim 36, wherein the computer readable medium is a memory, random-access-memory, read-only-memory, disk drive, or CD-ROM.

38. A computer system for encrypting data packets, comprising:

a processor;

a computer readable medium coupled to the processor storing a computer program comprising:

computer code that receives a data packet from a source for a destination, the data packet including a header section and a data section, and the header section storing a source identifier and a destination identifier;

computer code that determines whether the data packet should be encrypted upon reference to at least one of the source and destination identifiers; and

computer code that encrypts the data packet to produce an encrypted data packet if the data packet should be encrypted.

39. The computer program product of claim 38, wherein the computer readable medium is a memory, random-access-memory, read-only-memory, disk drive, or CD-ROM.

40. A method of decrypting data packets, comprising:

receiving a data packet from a source for a destination, the data packet including a header section and a data section, and the header section storing a source identifier and a destination identifier;

determining whether the data packet is encrypted upon reference to at least one of the source and destination identifiers; and

if the data packet is encrypted, decrypting the data packet to produce a decrypted data packet.

41. The method of claim 40, further comprising transmitting the decrypted data packet to the destination.

42. The method of claim 40, wherein the determining whether the data packet is encrypted comprises accessing stored information that indicates by presence or absence of the source identifier that data packets from the source are encrypted.

43. The method of claim 40, wherein the determining whether the data packet is encrypted comprises accessing stored information that indicates by presence or absence of a correlation between the source and destination identifiers that data packets from the source for the destination are encrypted.

44. The method of claim 40, wherein the data section of the data packet includes an encrypted header section and an encrypted data section for the decrypted data packet.

45. The method of claim 44, wherein the encrypted header section stores the source and destination identifiers.

46. The method of claim 44, wherein the source is a network and the encrypted header section stores an identifier of a host computer in the network.

47. The method of claim 44, wherein the destination is a network and the encrypted header section stores an identifier of a host computer in the network.

48. The method of claim 40, wherein the source is a host computer or a network.

49. The method of claim 40, wherein the destination is a host computer or a network.

50. A computer program product for decrypting data packets, comprising:

computer code that receives a data packet from a source for a destination, the data packet including a header section and a data section, and the header section storing a source identifier and a destination identifier;

computer code that determines whether the data packet is encrypted upon reference to at least one of the source and destination identifiers;

computer code that decrypts the data packet to produce a decrypted data packet if the data packet is encrypted; and

a computer readable medium that stores the computer codes.

51. The computer program product of claim 50, wherein the computer readable medium is a memory, random-access-memory, read-only-memory, disk drive, or CD-ROM.

52. A computer system for decrypting data packets, comprising:

a processor;

a computer readable medium coupled to the processor storing a computer program comprising:

computer code that receives a data packet from a source for a destination, the data packet including a header

section and a data section, and the header section storing a source identifier and a destination identifier;

computer code that determines whether the data packet is encrypted upon reference to at least one of the source and destination identifiers; and

computer code that decrypts the data packet to produce a decrypted data packet if the data packet is encrypted.

53. The computer program product of claim 52, wherein the computer readable medium is a memory, random-access-memory, read-only-memory, disk drive, or CD-ROM.